UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/922,041	08/03/2001	Larry H. Gass	ITL.0506US (P10475)	7270

21906 7590 06/25/2008

TROP PRUNER & HU, PC
1616 S. VOSS ROAD, SUITE 750
HOUSTON, TX 77057-2631

EXAMINER	
NGUYEN, MINH DIEU T	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
06/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/922,041
Filing Date: August 03, 2001
Appellant(s): GASS ET AL.

Timothy N. Trop
Registration Number: 28,994
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 4/10/2008 appealing from the Office action mailed 11/16/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

This appeal involves claims 1, 3-7, 27, 29, 32 and 40-42.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,976,163	Hind et al.	12-2005
5,748,940	Angelo et al.	5-1998
2002/0166061	Falik et al.	11-2002
2001/0050990	Sudia	12-2001
2002/0138592	Toft	9-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 33-35 and 38-41 are rejected under 35 U.S.C. 102(e) as being anticipated by Hind et al. (6,976,163).

a) As to claim 33, Hind discloses a method comprising storing a first portion of a firmware code which is not upgradable in a first reprogrammable semiconductor memory (i.e. permanent and non-modifiable content is stored in read only memory 240,

Hind: col. 8, lines 41-44); providing a second portion of a firmware code that is upgradable in said first reprogrammable semiconductor memory (i.e. semi-permanent and modifiable are in the programmable memory 236, Hind: col. 8, lines 37-41); and providing information for authenticating an upgrade of the second portion in the first portion (Hind: col. 3, lines 47-49; col. 8, lines 57-60). Hind further discloses a single memory array may be utilized to provide the programmable memory, the read only memory and the system memory (Hind: col. 9, lines 30-33), as such the first portion and second portion of a firmware code can be in a single memory.

b) As to claim 34, Hind discloses locking the first portion to prevent reading said first portion (i.e. preventing read operations to the ROM, Hind: col. 7, lines 35-53).

c) As to claims 35 and 38, Hind discloses providing a signature authentication in said first portion and providing instructions in said first portion to confirm the validity of a firmware upgrade file (Hind: col. 8, lines 57-60; col. 10, lines 54-67).

d) As to claim 39, Hind discloses determining whether an upgrade request is authentic and if said upgrade request is not authentic, locking the second portion against being written (Hind: col. 12, lines 45-55).

e) As to claim 40, this claim is directed to a hardware implementation of the method of claim 33 and is rejected by a similar rationale applied against claim 33.

f) As to claim 41, Hind discloses a public key is included in said second portion (Hind: col. 12, lines 22-32).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 5-7, 27 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (5,748,940) in view of Falik et al. (2002/0166061) and further in view of Sudia (2001/0050990).

a) As to claims 1 and 27, Angelo discloses a secure updating of non-volatile memory comprising identifying a firmware upgrade request by a firmware program (i.e. a flash bit set to indicate a flash update will occur, Angelo: col. 3, lines 3-6); retrieving a file signed with a private key (Angelo: Fig. 3, element 310); validating a file with a public key (Angelo: Fig. 3, element 312; col. 3, lines 39-52); upgrading a portion of the firmware program (Angelo: Fig. 3, element 316).

Angelo does not disclose locking a device storing the firmware program such that a second portion of the firmware program is not readable.

Falik discloses an apparatus and method for protecting the contents of a shared memory in a memory device comprising a step of locking a device storing the firmware program such that a second portion of the firmware program is not readable (Falik: page 2, paragraph [0015]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of locking device storing the firmware program such that a

second portion of the firmware program is not readable in the system of Angelo, as Falik teaches, so as to prevent access to the firmware by unauthorized users.

Angelo and Falik do not disclose the steps of validating the public key and retrieving a second public key from the firmware program if the public key is not valid.

Sudia discloses a cryptographic system and method for upgrading device firmware (Abstract) of a trusted device comprising validating the public key and retrieving a second public key from the firmware program if the public key is not valid (Sudia: page 22, paragraph [0251]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of validating the public key and retrieving a second public key from the firmware program if the public key is not valid in the system of Angelo and Falik as Sudia teaches so as to efficiently perform firmware upgrade request.

b) As to claim 3, the combination of Angelo, Falik and Sudia discloses identifying a firmware upgrade request by a firmware program further comprising reading a flag, wherein the flag is located in a non-volatile medium (Angelo: Fig. 1, element 120; i.e. flash bit) and determining that the flag is set (Angelo: col. 2, lines 6-8).

c) As to claims 5 and 29, the combination of Angelo, Falik and Sudia discloses locking flags is utilized to implement software protection for each flash memory device blocks (Falik: page 1, paragraph [0014]; i.e. determining that the file is not authentic and locking the device).

d) As to claim 6, the combination of Angelo, Falik and Sudia discloses locking the device after upgrading a portion of the firmware program by the firmware program (Falik: page 9, paragraph [0111]; page 11, paragraph [0122]).

e) As to claim 7, the combination of Angelo, Falik and Sudia discloses the second portion of the firmware program is a public key (Angelo: col. 3, lines 39-52).

Claims 4 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Angelo et al. (5,748,940) in view of Falik et al. (2002/0166061) in view of Sudia (2001/0050990) and further in view of Toft (2002/0138592).

a) As to claim 32, Angelo discloses a secure updating of non-volatile memory comprising identifying a firmware upgrade request by a firmware program (i.e. a flash bit set to indicate a flash update will occur, Angelo: col. 3, lines 3-6); retrieving a file signed with a private key (Angelo: Fig. 3, element 310); validating a file with a public key (Angelo: Fig. 3, element 312; col. 3, lines 39-52); upgrading a portion of the firmware program (Angelo: Fig. 3, element 316).

Angelo discloses identifying a firmware upgrade request by a firmware program further comprising reading a flag, wherein the flag is located in a non-volatile medium (Angelo: Fig. 1, element 120; i.e. flash bit) and determining that the flag is set (Angelo: col. 2, lines 6-8).

Angelo does not disclose locking a device storing the firmware program such that a second portion of the firmware program is not readable.

Falik discloses an apparatus and method for protecting the contents of a shared memory in a memory device comprising a step of locking a device storing the firmware program such that a second portion of the firmware program is not readable (Falik: page 2, paragraph [0015]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of locking device storing the firmware program such that a second portion of the firmware program is not readable in the system of Angelo as Falik teaches so as to prevent access to the firmware by unauthorized users.

Angelo and Falik do not disclose the steps of validating the public key and retrieving a second public key from the firmware program if the public key is not valid.

Sudia discloses a cryptographic system and method for upgrading device firmware (Abstract) of a trusted device comprising validating the public key and retrieving a second public key from the firmware program if the public key is not valid (Sudia: page 22, paragraph [0251]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of validating the public key and retrieving a second public key from the firmware program if the public key is not valid in the system of Angelo and Falik as Sudia teaches so as to efficiently perform firmware upgrade request.

Angelo, Falik and Sudia do not explicitly disclose the steps of deleting the file and clearing the flag.

Toft discloses clearing the update flag before rebooting the system (Toft: paragraph [0022]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of clearing the update flag in the system of Angelo, Falik and Sudia asToft teaches so as to properly control the update process.

Angelo, Falik, Sudia and Toft do not explicitly disclose deleting the file.

The examiner takes official notice that deleting the upgrade file after it is being used is a common practice to save system memory.

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of deleting the file in the system of Angelo, Falik, Sudia and Toft so as to save system memory.

b) As to claim 4, please see addressed above claim 32.

Claims 36-37 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (6,976,163) in view of Sudia (2001/0050990).

Hind discloses a public key is provided in the second portion (Hind: col. 12, lines 22-32), however Hind is silent on the capability of having two public keys (claims 36 and 42) and two identical public keys (claim 37).

Sudia is relied on for the teaching of having two public keys and they are identical (Sudia: paragraphs [0251]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having two public keys and two identical public keys in the system of Hind as Sudia teaches so as to provide a back up key in the case the other key is lost or stolen (i.e. not valid).

(10) Response to Argument

a) Appellant, on page 11 of the brief, argues that the limitation "the first portion to store an upgrade verification code" is not addressed and Hind does not teach that limitation.

As indicated in the previous office action, claim 40 is directed to a hardware implementation of the method of claim 33 and is rejected by a similar rationale applied against claim 33, wherein "the first portion to store an upgrade verification code" is addressed in claim 33 as providing information for authenticating an upgrade of the second portion in the first portion (lines 4-5 on page 4 of office action dated 11/16/2007). Hind discloses firmware updates are needed after manufacture to enable new capabilities or to fix problems (Hind: col. 2, lines 3-9), as such the authenticity of the update image may need to be verified by means of a shared secret, or by a public-key cryptosystem. The verification of the image may be accomplished by including and checking a digital signature comprising a hash of the image encrypted by the private key of an update authority (Hind: col. 3, lines 18-26). Hind also discloses the certificate authority's public key which contained in the ROM (Hind: col. 3, lines 47-49) and an update control program to verify a digital signature of an update image (Hind: col. 8, lines 57-60). The combination of the certificate public key and the update control program being used together facilitates the process of verifying updated (upgraded) code. As such, Hind does teach the limitation of "the first portion to store an upgrade verification code".

b) Appellant, on page 11 of the brief, argues that the combination of Angelo, Falik and Sudia does not teach "retrieving a second public key from the firmware program if the public key is not valid".

Sudia is relied on for the teaching of "retrieving a second public key from the firmware program if the public key is not valid". Sudia discloses multiple instruction keys (i.e. second public key) of the trusted third parties in the device firmware besides the manufacturer's signature key (i.e. public key). Sudia further teaches the manufacturer's key is compromised, lost or destroyed which would make the key not valid. If one of these conditions occurs, then the trusted third party's instruction key can be used to replace to efficiently provide a recovery system (Sudia: 0251).

c) Appellant, on page 11 of the brief, argues the same issue as submitted in section b).

On the same basis as explained above in section b), the rejections of claims 4 and 32 are maintained.

d) Appellant, on page 11 of the brief, argues the same issue as submitted in section a).

On the same basis as explained above in section a), the rejections of claim 42 is maintained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Minh Dieu Nguyen/

Primary Examiner, Art Unit 2137

June 17, 2008

Conferees:

Emmanuel L Moise

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137

Matthew B. Smithers

/Matthew Smithers/
Primary Examiner, Art Unit 2137